



Office of the Inspector General U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats

REDACTED FOR PUBLIC RELEASE

The full version of this report contains information that the Department considered to be classified and therefore could not be publicly released. To create this public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.

Audit Division 19-18

March 2019



SECRET//NOFORN//SSI

(U) EXECUTIVE SUMMARY

(U) Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats

(U) Objectives

(U) The Department of Justice Office of the Inspector General conducted an audit of the Federal Bureau of Investigation's (FBI) roles and responsibilities for:

- (1) assessing Maritime terrorism threats and
- (2) coordinating with the Department of Homeland Security (DHS) components in ensuring seaport security. Unless otherwise stated, the audit focused on activities from October 2012 through July 2017.

(U) Results in Brief

(U) Although FBI officials told us they consider the terrorism threat to the Maritime domain to be low, we believe this assessment is based on incomplete and potentially inadequate information. Our review determined that the FBI does not conduct its own, formal Maritime threat assessment and the informal assessments made by the FBI have not included all information available to the FBI. For example, we found that many Maritime-related incidents with a potential nexus to terrorism were not coded as such in the FBI's threat database and relevant search terms were omitted from database queries.

(S) We also found significant deficiencies related to the FBI's role in providing information to the Transportation Security Administration (TSA) in support of the TSA's Transportation Worker Identification Credential (TWIC) program, which provides cardholders unescorted access to secure Maritime facilities and vessels. We concluded that the FBI has [REDACTED]

[REDACTED] despite the risk to Maritime security. Yet, some FBI agents we spoke with who provided input to the TSA did not adequately understand the level of access provided by a TWIC or other crucial details about the program and its risks.

(U) Finally, we found that the FBI's Maritime Security Program unit does not receive information related to TWIC Terrorist Watchlist encounters, which prevents it from identifying security threats and trends.

(U) Recommendations

(U) Our report contains 9 recommendations to strengthen the FBI's Maritime counterterrorism activities.

(U) Audit Results

(U) As our Nation's lead counterterrorism agency, the FBI is responsible for investigating terrorism and related criminal activity in the Maritime domain, as well as gathering and sharing intelligence with key stakeholders. In carrying out its responsibilities, the FBI coordinates with three primary DHS components: the United States Coast Guard (USCG), Customs and Border Protection (CBP), and the TSA. The USCG has general law enforcement authority in the Maritime domain, the CBP is responsible for inspecting persons and cargo that enter the United States through its ports, and the TSA is responsible for ensuring individuals who require access to secure Maritime facilities, vessels, and critical infrastructure are thoroughly vetted.

(U) FBI's Intelligence Assessment of Maritime Terrorism Threats – Based on our review, the FBI has not conducted its own formal Maritime terrorism threat assessment. However, the FBI's Assistant Director over its Counterterrorism Division along with the Unit Chief over its Maritime Security Program (MSP) told us they view the threat of terrorism in the Maritime area as being low. These officials told us their views were based on the: (1) small number of Maritime-related incidents in Guardian, the FBI's terrorism threat management system; (2) small number of resulting investigations; and (3) lack of a prior domestic Maritime-related terrorism attack. However, we found that the FBI officials' views may not have been informed by all relevant information available to the FBI. For example, we found that the FBI did not identify within Guardian some incidents as "Maritime-related," nor did MSP personnel utilize certain Maritime-related keywords in its searches of Guardian and other available systems. Further, we believe that MSP personnel lacked crucial knowledge about the access a TWIC card provides to Maritime facilities and vessels, and other aspects of the program and its risks. Consequently, FBI personnel may not have had a complete picture of Maritime vulnerabilities and threats when assessing Maritime risks. We recommend that the FBI conduct its own independent Maritime threat assessment, which we believe would help the FBI ensure that it has a comprehensive understanding of Maritime-related terrorism threats and vulnerabilities.

SECRET//NOFORN//SSI



SECRET//NOFORN//SSI

(U) EXECUTIVE SUMMARY

(U) Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats

(S//SSI) The FBI's Role in the TWIC Vetting Process and TWIC Terrorist Watchlist Encounters

— [REDACTED]. Consequently, TSA asks the FBI to make recommendations about whether to approve or reject TWIC card applications from KSTs, who if approved would have unescorted access to secure Maritime facilities and vessels. We found that between January 2008 and January 2017, the [REDACTED] or had already issued a TWIC card to at least [REDACTED] watchlisted individuals. These individuals included a [REDACTED], individuals known to have [REDACTED], and a [REDACTED]. Of these, [REDACTED] were known or suspected terrorists (KST) and on the No Fly list. We concluded that in the large majority of applications we reviewed involving KSTs, the FBI had [REDACTED].

(U) However, FBI Agents we spoke to who provided input on these individuals did not adequately understand the TWIC program and its risks. For example, some Agents were unable to explain what a TWIC was and what access it granted, and others had not fully considered the impact of allowing an investigative subject continued access to secure Maritime areas. Moreover, our review of FBI documentation found few instances where mitigating FBI actions, such as physical surveillance, were noted.

(U) We also found that FBI personnel were not adequately retaining their communications with the TSA concerning TWIC decisions. Without this important information, the FBI failed to maintain a thorough record of actions and information on Terrorist Watchlist-nominated individuals who sought access to secure Maritime facilities through a TWIC card.

(U) Additionally, MSP, organizationally located within the FBI's Counterterrorism Division and the National Joint Terrorism Task Force, is tasked with preventing, penetrating and dismantling acts of terrorism directed against Maritime assets. However, the MSP was not directly notified of information on TWIC encounters of watchlisted individuals, which we believe inhibits MSP's ability to facilitate intelligence sharing and identify terrorism-related trends in the Maritime realm.

(U) Further, we believe that the FBI should strengthen its policies and procedures for working with the TSA to enhance the vetting and increase scrutiny of TWIC applicants and cardholders with a Terrorist Watchlist status, especially those with a "No Fly" status. Specifically, the FBI can improve how it makes its recommendations to the TSA, maintains records related to those recommendations, and incorporates the MSP in the information sharing process.

(U//SSI) Access to Secure Areas of Ports and Maritime Facilities – While the USCG is responsible for the enforcement of TWIC cards at the ports, the FBI has the important responsibility of investigating terrorism threats and gathering related intelligence, including KSTs' attempts to gain access to secure Maritime areas. However, our audit identified concerns that complicate the FBI's ability to fulfill this important responsibility. For example, [REDACTED] use only visual inspections of TWIC cards and therefore do not use the biometric and electronic security features contained in the card. As of May 2017, the USCG could not provide the number of ports with electronic card readers. We also identified 29 instances of lost, stolen, misused, or counterfeited TWIC cards, many of which had not been coded in Guardian as "Maritime-related." We believe the FBI must remain cognizant of and routinely consider these and other vulnerabilities when assessing the Maritime threat, and to this end we make recommendations to assist MSP in improving its process for planning, selecting, and summarizing its port visits.

(U) In light of the responsibilities of TSA, USCG, and CBP in the Maritime domain, we have shared the findings and conclusions of this audit with our counterparts at DHS OIG.

SECRET//NOFORN//SSI

**(U) AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S
MANAGEMENT OF MARITIME TERRORISM THREATS**

(U) TABLE OF CONTENTS

(U) INTRODUCTION	1
(U) OIG Audit Approach	2
(U) AUDIT RESULTS	4
(U) FBI's Intelligence Assessment of Maritime Terrorism Threats	4
(U) FBI's Role in TSA's TWIC Vetting Process	8
(U) TWIC Application and Terrorist Watchlist Encounters	10
(U) Individuals on the No Fly List Who Held Active TWICs at the Time of Encounter	11
(U) Post-Encounter FBI Coordination with Maritime Stakeholders	14
(U) Access to Secure Areas of Ports and Maritime Facilities	16
(U) CONCLUSION AND RECOMMENDATIONS	20
(U) STATEMENT ON INTERNAL CONTROLS	22
(U) STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS	23
(U) APPENDIX 1: OBJECTIVES, SCOPE, AND METHODOLOGY.....	24
(U) APPENDIX 2: TWIC DISQUALIFYING OFFENSES.....	26
(U) APPENDIX 3: LIST OF KEYWORDS FOR MSP SEARCHES	27
(U) APPENDIX 4: FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT	28
(U) APPENDIX 5: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT	31

(U) AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF MARITIME TERRORISM THREATS

(U) INTRODUCTION

(U) According to the Maritime Operational Threat Response Plan, one of the eight supporting implementation plans of the National Strategy for Maritime Security, the coordinated U.S. government response to threats against the United States and its interests in the Maritime domain is a shared responsibility at the federal level to include the FBI and the Department of Homeland Security (DHS). Specifically, the DHS components with Maritime-related responsibilities include the United States Coast Guard (USCG), Customs and Border Protection (CBP) and Transportation Security Administration (TSA).^{*1} The FBI, as the lead agency for investigating terrorist activities, is responsible for investigating terrorism and related criminal threats and activity in the Maritime domain, as well as gathering and sharing intelligence with key stakeholders. The USCG has law enforcement authority in the Maritime domain, the CBP is responsible for inspecting persons and cargo that enter the United States through its ports, and the TSA ensures that individuals who require access to the nation's secure Maritime facilities and vessels are thoroughly vetted.² In addition to the federal level, state and local law enforcement also play a role in port security, specifically as first responders to Maritime incidents.

(U) In 2005, the FBI created the Maritime Security Program (MSP) which is a part of its National Joint Terrorism Task Force (NJTTF) within the Counterterrorism Division and functions as its Maritime counterterrorism intelligence unit. According to the FBI, the mission of the FBI's MSP is to "prevent, penetrate, and dismantle criminal acts of terrorism directed against Maritime assets and provide counterterrorism preparedness leadership and assistance to federal,

^{*}(U) WARNING: This report contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. The Sensitive Security Information in this report may not be disclosed to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration (TSA) or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Parts 15 and 1520.

¹ (U) Maritime ports refer to ports along navigable waterways, such as sea and river. According to the Maritime Transportation Security Act of 2002, there are over 360 ports in the United States.

(U) The MOTR Plan was an effort across government agencies to create a National Strategy for Maritime Security in 2006. The most recent update to the MOTR protocol, a supplement to the MOTR Plan, occurred in June 2014.

² (U) National Security Presidential Directive-41 (NSPD-41) and Homeland Security Presidential Directive-13 (HSPD-13) defines the Maritime domain as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all Maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances." NSPD-41 and HSPD-13, December 21, 2004.

state, and local agencies" responsible for Maritime security. As of May 2018, the MSP had a staff of one FBI agent and two intelligence analysts (one from the FBI and one from DHS). These MSP personnel compile Maritime-related intelligence from multiple sources and disseminate that information to FBI field office personnel designated as Maritime Liaison Agents (MLA). MLAs, who are also assigned to field offices and JTTFs, primarily conduct liaison responsibilities with key Maritime partners and industry.

(U) The NJTTF established the Maritime Liaison Agent program that is comprised of FBI Agents and JTTF officers operating in field offices with navigable waterways. According to the FBI, the purpose of the MLA program is to enhance the security of the Maritime environment through increased interaction between MLAs, state and local authorities, and other federal agencies with Maritime responsibilities, including national security stakeholders and private industry. Further, the MSP personnel coordinate training for MLAs and conduct port visits.

(U) An important part of protecting ports is controlling access to the ports, vessels, and other Maritime facilities located within the port. Without proper controls, a terrorist network could commit violent acts resulting in loss of life, as well as structural or economic damage. The FBI's sharing of intelligence regarding high risk individuals' efforts to gain access to secure Maritime areas with Maritime security stakeholders can provide vital information to entities making important decisions regarding Maritime security. Therefore, the FBI must work with other agencies, such as the USCG, CBP, and the TSA, to ensure that only those with legitimate reasons have access to these critical facilities and those with nefarious purposes are prohibited and duly investigated.

(U) OIG Audit Approach

(U) The objectives of the audit were to review the FBI's roles and responsibilities for: (1) assessing Maritime terrorism threats and (2) coordinating with the Department of Homeland Security (DHS) components in ensuring seaport security. The scope of this audit, unless otherwise stated, generally focused on activities from October 2012 through July 2017.

(U) In conducting this audit, we completed work at the FBI and at other agencies with port and Maritime security responsibilities, including the USCG, CBP, and TSA. At the FBI, we conducted interviews with personnel at the MSP, the Critical Incident Response Group, the Criminal Investigative Division, and the Directorate of Intelligence Division. We also interviewed MLAs in Long Beach, Monterey, and San Francisco, California and personnel in other FBI field offices across the country.

(U) Further, we met with DHS officials at the Global Maritime Operational Threat Response Coordination Center, the USCG, the CBP, and the TSA. More specifically, we completed fieldwork at the USCG's Coastwatch, and interviewed the Captain of the Port in San Francisco, California and personnel in the Port of Los

Angeles. At the CBP, we conducted fieldwork at the National Targeting Center and the Information and Incident Coordination Unit in Washington, D.C. Further, we spoke with personnel from TSA's Transportation Worker Identification Credential (TWIC) program. Further, in light of the responsibilities of TSA, USCG, and CBP in the Maritime domain, we have shared the findings and conclusions of this audit with our counterparts at DHS OIG periodically throughout the audit.

(U) Our report contains 9 recommendations to strengthen the effectiveness of the FBI's actions to protect the Maritime domain.

(U) AUDIT RESULTS

(U) We found that although the FBI has not conducted its own formal Maritime terrorism threat assessment, key FBI counterterrorism officials viewed the threat of terrorism in the Maritime area as being low. This unwritten assessment was based on the small number of Maritime-related incidents and investigations identified in the FBI's threat database, as well as the lack of a prior Maritime-related terrorism attack. However, we believe this assessment was based on incomplete and potentially inadequate information because the MSP's process for reviewing threat data failed to identify all Maritime-related threats. The MSP cannot make a well informed determination of the overall Maritime terrorism threat without complete and adequate information and it may not be disseminating all relevant information to MLAs and FBI field offices.

(~~S//SSI~~) In addition, we found that the FBI plays a critical role in the TSA-administered Transportation Worker Identification Credential (TWIC) program by sharing intelligence regarding watchlisted individuals when they apply for or attempt to renew a TWIC. Obtaining a TWIC allows these individuals unescorted access to secure Maritime facilities. We identified significant deficiencies related to the FBI's role in this area. Specifically, we found that FBI personnel provided guidance to the TSA on TWIC applications without having an adequate understanding of the credential program and its risks. This is concerning because TSA officials [REDACTED]. We also found the FBI lacks comprehensive policies and procedures for its coordination with the TSA regarding TWIC applications, and it did not adequately maintain documentation of its communications with TSA.

(U) Additionally, the FBI has no established formalized procedures for communicating TWIC encounter information to the MSP.³ We also found the FBI is not fully aware of some port security measures, such as the number and location of ports using only a visual inspection of TWIC cards.

(U) FBI's Intelligence Assessment of Maritime Terrorism Threats

(U) We found that the FBI has not conducted its own formal Maritime terrorism threat assessment.⁴ Nevertheless, the FBI's Assistant Director for the Counterterrorism Division and the Unit Chief responsible for MSP told us that the terrorism threat risk to the Maritime domain is low. FBI officials cited the small number of Maritime-related incidents entered into its Guardian system and the few

³ (U) Throughout this report, the encounters we describe are all the result of a watchlisted individual applying or re-applying for a TWIC card, or of TWIC program recurrent vetting.

⁴ (U) The Program Manager of MSP stated that the Counterterrorism Division does not normally assess domains or other critical infrastructure but rather focuses on known terrorist groups.

Maritime-related terrorism investigations as support for their assessment.⁵ Additionally, these officials cited the lack of a domestic Maritime-related terrorism attack and that the primary responsibility for protecting the nation's ports and making informed assessments on Maritime terrorism threats rests with the USCG rather than the FBI. For example, FBI officials stated that the MSP does not conduct assessments on Maritime terrorism threats. FBI officials also stated that although the FBI's Directorate of Intelligence and specific FBI Field Offices may produce Maritime-specific intelligence products related to criminal activity, including terrorism on a case-by-case basis, the USCG has the primary responsibility for making informed assessments on Maritime terrorism threats.

(U) However, we found that the FBI officials' assessment lacked available information. As the FBI's system for managing terrorist threats and reports of suspicious activities, Guardian is intended to ensure that all reported threats to U.S. persons and interests and suspicious activities with a potential nexus to terrorism are investigated. The data in Guardian allows for the analysis of trends and patterns of threats and suspicious activity, including those related to the Maritime domain. As described below, we found 10 TWIC-related incidents that were not appropriately categorized as Maritime or Transportation in Guardian as they should have been, and therefore that the FBI may not have been aware of all relevant information it would need to make a determination that the Maritime threat risk is low. Towards the end of our fieldwork in May 2018, FBI officials stated that in November 2017 the NJTTF began to conduct daily Guardian review compliance audits to ensure proper tagging of all six NJTTF sectors including Maritime-related threats.

(U) FBI policy states that each Guardian threat should be investigated to determine if there is a nexus to terrorism and, if so, the FBI should initiate a Full or Preliminary Investigation. Analysts at the FBI's Guardian Management Unit (GMU) review Guardian incident data and issue quarterly reports discussing concerns and trends identified in the critical infrastructures such as Transportation and Maritime. Additionally, MSP personnel search Guardian data to obtain Maritime-related intelligence to share with MLAs and other Maritime security stakeholders in the field.

⁵ (U) Launched in 2004, Guardian is the FBI's incident reporting and management system that collects, stores, and manages terrorist threats and reports of suspicious activities. A Guardian incident is a reporting of a threat or suspicious activity with either a known or perceived potential nexus to terrorism. Threats and reports of suspicious activities are entered into Guardian by the FBI, Joint Terrorism Task Force (JTTF) officers, or by local law enforcement through eGuardian. The FBI's Counterterrorism Policy Guide requires that all incidents with a potential nexus to terrorism be entered into Guardian. Other government and law enforcement agencies may enter information into eGuardian, an unclassified system, if they have an account. Incidents entered into eGuardian are forwarded to the nearest state fusion center, or if none exists within the area of the submitting entity, to the Guardian Management Unit (GMU) for approval to be entered into Guardian.

(U) We requested and obtained data related to overall Guardian incidents for FYs 2013 through 2016, as well as incidents related to the Transportation sector and Maritime, a subsector of Transportation. We requested data on Guardian incidents categorized as "Transportation" and specific to the subcategory "Maritime" for FYs 2013 through 2016.⁶ As illustrated in Table 1, the total number of Maritime-specific Guardian incidents for FYs 2013 through 2016 was 869, which is less than 1 percent of all Guardian incidents and approximately 9 percent of the Transportation category of Guardian incidents.

(U) Table 1
Maritime-related Guardian Incidents for FYs 2013 through 2016

Fiscal Year	Number of All Guardian Incidents	Number of Maritime-specific Guardian Incidents	Maritime Incidents determined to have Nexus to Terrorism
2013	19,217	207	Unavailable ^a
2014	18,542	220	2
2015	23,613	220	7
2016	29,879	222	6
Total	91,251	869	15

^a FBI officials said that FY 2013 disposition data was unavailable due to the way information was captured and stored prior to FY 2014.

(U) Source: OIG analysis of FBI data.

(U//~~SSI~~) Maritime-specific Guardian threats that result in investigations are rare, accounting for approximately 2 percent of all Maritime-related Guardian incidents. Between FY 2014 and FY 2016, the FBI initiated Full or Preliminary Investigations for 15 Maritime-related Guardian incidents determined to have a nexus to terrorism.⁷ Bomb threats, persons of interest, and Maritime laser incidents accounted for [REDACTED] of these incidents. The remaining incidents related to a variety of activity such as a cargo radiation alarm, suspicious photography, concerning activity on social media, and a suspicious call to a shipping company.

⁶ (U) The FBI's Guardian Management Unit (GMU) Analysts categorize all Guardian incidents to 1 of 16 critical infrastructures and a subcategory, if appropriate. "Maritime" is a subcategory of the "Transportation" critical infrastructure. The "Maritime" subcategory includes incidents relating to Commercial Vessels, Cruise Ships, Drilling Platforms, Ferries, Military Vessels, Port Facilities, and Tankers. The capability to assign incidents to these critical infrastructures and subcategories was created in 2014.

(U) As of September 2017, the MSP Program Manager stated that the GMU no longer exists. In February 2018, the MSP Program Manager stated that NJTTF personnel review all Guardian incidents and assign "incident tags" specific to programs within the NJTTF, such as Maritime, Aviation, and Railroad.

⁷ (U) As of August 2017, 6 of these 15 FBI investigations were still pending and the remaining 9 cases have been closed.

(~~S//NF//FOUO//SSI~~) Despite their apparent rarity, Maritime-specific Guardian incidents with a nexus to terror can be potentially significant. For example, [REDACTED] of these [REDACTED] instances was a [REDACTED] encounter with a KST.⁸ This Maritime Guardian encounter related to a KST who was on the No Fly list. [REDACTED]

[REDACTED]. Fortunately, because of the intelligence gathered at [REDACTED], the FBI was able to interview him upon his arrival in [REDACTED].

(U//~~SSI~~) Moreover, we believe the low number of Maritime Guardian incidents does not provide an accurate and complete picture of the threat to the Maritime domain. We identified [REDACTED] Guardian records associated with TWIC-related encounters that were not categorized as Transportation or Maritime.⁹ [REDACTED] of these [REDACTED] individuals were KSTs who required additional screening prior to boarding flights, which indicates an increased risk to transportation. [REDACTED] of the [REDACTED] individuals had active TWICs at the time of the encounter. Yet the related Guardian records created following the encounters were not included in either Transportation or Maritime Guardian data, and thus would not be identified by MSP's database checks. While we only found a small number of instances where this occurred, the risk these watchlisted individuals pose to the nation's Maritime activity therefore would not be included in FBI trend analysis of Guardian data specific to Transportation and Maritime and reliance on incomplete information can pose a significant threat to the Maritime domain.

(U) Further, MSP Analysts perform keyword searches of the Guardian system to identify Maritime-related intelligence leads for inclusion in their Intelligence Summary Reports to field personnel.¹⁰ We reviewed a list of the keywords MSP personnel use to understand the current process for obtaining Maritime-related intelligence information.¹¹ We noted the absence of "TWIC" and "Transportation Worker Identification Credential," in addition to several other relevant terms, such as "submersible," "submarine," and "stowaway."¹²

⁸ (U//~~FOUO~~) The [REDACTED] is the unit within the Terrorist Screening Center that contacts FBI Case Agents regarding positive encounters.

⁹ (U//~~SSI~~) Of these [REDACTED] Guardian incidents, [REDACTED] were not categorized, [REDACTED] were categorized under "Individuals & Groups Sector" and [REDACTED] was categorized under "Border & Immigration Section."

¹⁰ (U) These reports are compiled through the use of various sources. MSP personnel noted that they query the Internet and open source systems from the following agencies in an effort to compile the most comprehensive reports: (1) National Counterterrorism Center, (2) National Security Agency, (3) Central Intelligence Agency, and (4) DHS components.

¹¹ (U) The list of these keywords is included in Appendix 3.

¹² (U) As described below, an MSP official also told us that MSP would not be contacted directly in the event of a TWIC encounter.

(U) We asked the GMU to search all Guardian incidents for the keyword "TWIC" and "Transportation Worker Identification Credential" for FYs 2014 to 2016. A total of 206 Guardian incidents resulted from this keyword search, of which 29 specifically related to lost, stolen, or counterfeit TWICs or unauthorized access with TWIC. Fifteen of these 29 Guardian incidents were not categorized as Maritime. While it is possible that MSP personnel may have identified a portion of these incidents based on other keywords currently used by MSP, adding the keywords "TWIC" and "Transportation Worker Identification Credential" to their keyword searches would increase the chances of identifying these Guardian incidents and any resultant emerging threats to secure areas of ports. After expressing our concerns with the keywords list during the audit, MSP personnel updated the list to include "TWIC," "submersible," and a few others. We believe the FBI should periodically assess what keywords may provide intelligence value to the MSP's efforts in the Maritime counterterrorism activities. Further, providing more complete intelligence to FBI field personnel, including MLAs, increases the FBI's overall awareness of threats and vulnerabilities within the Maritime domain.

(U) Notably, MSP personnel stated that they do not have policies and procedures governing their keyword searches and the compilation of its Intelligence Summary Reports. We believe that formalizing the policies and procedures used for the MSP's keyword searches and preparing its Intelligence Summary Reports will facilitate the FBI providing more comprehensive intelligence to Maritime security stakeholders in the field and preserve continuity in the event of MSP personnel changes.

(U) Based on the foregoing, we believe the MSP does not currently identify all TWIC intelligence, and therefore does not have the information it needs to develop a complete understanding of the terrorism threat to the Maritime domain. Therefore, we recommend that the FBI conduct a full and independent evaluation, updated on a periodic basis, of the terrorism threat to the Maritime domain with resulting intelligence product(s) disseminated to key stakeholders. We further recommend that the FBI document the policies and procedures MSP personnel utilize to complete their Intelligence Summary Reports, such as listings of keyword searches and distribution lists, to ensure continuity of operations within the MSP and to ensure dissemination of the most thorough Maritime-related intelligence to field personnel.

(U) FBI's Role in TSA's TWIC Vetting Process

(U) The Maritime Transportation Security Act of 2002 (MTSA) established a requirement that all individuals with a need for unescorted access to secure Maritime facilities and vessels and authorized by each port's security plan hold a transportation security card. The TSA's TWIC is a tamper-and counterfeit-resistant biometric smart card credential valid for up to five years which provides authorized individuals, such as port and railroad workers and truck drivers, unescorted access

to secure MTSA-regulated port vessels and facilities.¹³ The management and enforcement of the TWIC program is under the purview of DHS agencies, specifically the TSA and the USCG. Our review generally focused on the FBI's role in the TSA's portion of the TWIC program to conduct a security threat assessment and issue a TWIC credential, given its responsibility for gathering intelligence on and investigating Maritime terrorist and related criminal activities.

(U) TWIC application data is compared against multiple databases, including the FBI's Next Generation Identification System and National Crime Information Center, TSA's Transportation Vetting System, and the FBI's Terrorist Screening Database (Terrorist Watchlist), to identify any criminal, immigration, and terrorism-related offenses.¹⁴ According to the TSA, the results of the comparisons to the various databases are taken into consideration when the TSA decides whether an individual should be granted a TWIC.¹⁵

(U//~~SSI~~) According to TSA officials, [REDACTED] Therefore, effective vetting and coordination between the FBI and the TSA is vital to mitigating the risk that terrorists could exploit the program to obtain access to secure areas in the Maritime domain. To that end, [REDACTED]
[REDACTED] In the following sections, we discuss the coordination between the FBI and the TSA with regard to watchlisted TWIC applicants.

¹³ (U) According to a September 2016 DHS OIG report, the "TSA embeds the Transportation Worker Identification Credential with an encrypted file containing a cardholder's name, photo, two fingerprints, and the expiration date of the credential." According to the DHS OIG as of October 2015, TSA had issued, "more than 3.5 million TWICs, including both initial cards and renewals, of which approximately 2.1 million unique cards were active." Department of Homeland Security Office of the Inspector General, *TWIC Background Checks are Not as Reliable as They Could Be*, OIG-16-128 (September 1, 2016). As of May 2018, TSA had issued more than 4.9 million TWICs, of which more than 2.2 million cards were active.

(U) Throughout this report, references to secure areas, facilities and vessels refer to secure MTSA-regulated Maritime areas, facilities and vessels.

¹⁴ (U) TWIC application data includes name, address, birthdate, country of birth, citizenship, criminal history, and other relevant data.

¹⁵ (U) Appendix 2 presents permanent and interim disqualifying criminal offenses for the TSA TWIC Program.

¹⁶ (U) Watchlisted individuals are required to undergo extra screening upon entering U.S. ports of entry and, when physically encountered at a port of entry, will be delayed by law enforcement or screening personnel for further vetting.

(U) TWIC Application and Terrorist Watchlist Encounters

(U//~~SSI~~) The TSA TWIC application vetting process includes a comparison of application information against the Terrorist Watchlist and other government databases. [REDACTED]

(U//~~SSI~~) [REDACTED], the TSC considers any possible match to the Terrorist Watchlist to be an "encounter." Any encounters are transmitted to the TSC, [REDACTED] to the Terrorist Watchlist, where personnel review each encounter to confirm whether it is a positive, negative, or inconclusive match.¹⁷ TSC personnel compare identifying information provided from the encounter, such as name, date of birth, and Social Security number, to a Terrorist Watchlist record to confirm if the person is on the Terrorist Watchlist or not.

(U//~~FOUO~~) When an encounter is positively identified as a Terrorist Watchlist match, the TSC forwards the encounter information to the assigned FBI Case Agent or, if the subject is not under FBI investigation, the TSC's policy requires the [REDACTED] to create a Guardian incident. If a Guardian incident is created, it is then transferred to the appropriate FBI field office. Additionally, [REDACTED] will notify FBI field offices and FBI Headquarters oversight units. All Guardian leads are assessed for potential terror threats and if there is a determination an incident is terror related, a preliminary investigation is opened.

(U//~~SSI~~) We requested information from the TSC on encounters from October 2006 through January 2017 with watchlisted individuals who either held or had applied for a TWIC.¹⁸ In all, based on TSA and TSC information, we determined there were 214 confirmed incidents of such an encounter during this time period. Through our analysis of the encounter information, we determined that the 214 confirmed encounters involved [REDACTED] unique individuals, [REDACTED] of whom had an active TWIC at the time of the encounter.¹⁹

¹⁷ (U) An inconclusive encounter occurs when the TSC is unable to determine if the individual encountered is a match to an individual on the Terrorist Watchlist.

¹⁸ (U) While this information was requested for FY 2006 through January 2017, the first encounter included in the data set was from FY 2008. According to the TSC, this was the first instance in which the TSA contacted the TSC for information on a TWIC applicant which resulted in a match to the Terrorist Watchlist. The documentation we reviewed contained information contemporaneous with the time of each specific encounter.

¹⁹ (U//~~SSI~~) [REDACTED] of these [REDACTED] individuals had multiple encounters within the time period reviewed.

(U//SSI) We reviewed Terrorist Watchlist nomination category information provided by the TSC and found that [REDACTED] of the [REDACTED] individuals were identified as [REDACTED], [REDACTED] were [REDACTED], and [REDACTED] had provided [REDACTED]. See Table 2 below for the nomination category information for all [REDACTED] individuals who held or had applied for a TWIC and had a nexus to terrorism at the time of the encounter.

(U) Table 2

(U) Individuals Who Held or Had Applied For a TWIC and Had a Nexus to Terrorism at the Time of Encounter

(U) 2008-2017

(U) Nexus to Terrorism	(U) No. of Individuals	(U) No. of Individuals with an Active TWIC
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED] ^a	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED]	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U//SSI) [REDACTED] ^a	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]
(U) Total	(U//SSI) [REDACTED]	(U//SSI) [REDACTED]

^a (U) Individuals in these categories were not on the Terrorist Watchlist because they do not meet the reasonable suspicion criteria to be designated a known or suspected terrorist.

(U) Source: OIG analysis of TSC records.

(U) Individuals on the No Fly List Who Held Active TWICs at the Time of Encounter

(U//SSI) Of the [REDACTED] watchlisted individuals with an active TWIC at the time of their encounter, we determined that [REDACTED] were designated with a No Fly status. Further, an additional [REDACTED] of the [REDACTED] individuals with an active TWIC were designated for [REDACTED] and [REDACTED] screening. These individuals undergo additional screening at airports, but not when entering secure areas in the Maritime domain because of their TWIC. To be assigned a No Fly status, the FBI must document sufficient derogatory information and predication of a threat to commercial aviation. An individual with a No Fly status generally cannot fly on

commercial aircraft for security reasons, yet those that hold a TWIC are afforded unescorted access to secure Maritime facilities.²⁰

(~~S//SSI~~) We reviewed Sentinel, Guardian, and Encounter reports to obtain an understanding of the risks posed by these [REDACTED] individuals.²¹ See Table 3 below for complete [REDACTED]. We note that many of these KSTs no longer hold their TWIC, have been removed from the No Fly list, or both.

(U) Table 3

(~~S//NF~~) [REDACTED]



(U) Source: OIG analysis of the FBI's records.

²⁰ (U) The FBI and the DHS do not have restrictions in the Maritime domain similar to the No Fly list for civil aviation; for example, there is no "No Float" list.

²¹ (U) Sentinel is a software case management system developed and used by the FBI.

(~~S//NF//SSI~~) The information we reviewed in FBI files about some of the individuals in Table 3 was particularly concerning. [REDACTED]

(~~S//NF//SSI~~) [REDACTED]

[REDACTED] These encounter records also indicate that the FBI's Domestic Terrorism Operations Unit (DTOU) prepared memoranda at that time indicating that the subjects were potential threats to transportation to the TSA, yet there is no evidence that the FBI actually provided these memoranda to the TSA, and our review of TSA and FBI documentation indicated that neither TWIC was revoked. In February 2013, these two individuals were removed from the Terrorist Watchlist, and as of July 2017, both individuals had active TWICs.

(S) While we find it concerning that the FBI did not make every effort to ensure that [REDACTED], we find it particularly concerning in the case of [REDACTED]

[REDACTED] Because of the TWIC, this individual had access to large scale modes of Maritime transportation and ports, [REDACTED], which served to increase the risk this individual posed to transportation. We recommend that the FBI strengthen its policies and procedures for working with the TSA to enhance the vetting and scrutiny of No Fly TWIC applicants and cardholders.

²² (U) The Lackawanna Six was a group of six individuals located near Buffalo, New York who were convicted of providing material support to Al-Qaeda in December 2003.

(U) Post-Encounter FBI Coordination with Maritime Stakeholders

(U) We reviewed the FBI's actions and coordination with the TSA in response to watchlisted individuals who applied for or who held active TWICs. The FBI and the TSA coordinate through memoranda to address the issuance and revocation of TWIC cards to watchlisted individuals. In our analysis, we found one instance of coordination and cooperation between the FBI, TSA, and USCG. For example, in one instance, the FBI, TSA, and USCG worked together to confiscate the active TWIC of an FBI investigative subject who should not have had access to secure Maritime areas. However, we also found that the FBI did not adequately maintain documentation of its communications with the TSA in response to TSA inquiries. We also found that FBI personnel may be providing guidance to TSA without having an adequate understanding of the TWIC card program. We discuss the FBI's post-encounter actions and coordination for FBI Watchlist-nominated individuals and watchlisted subjects of FBI investigations in the sections below.

(U) Encounters with FBI Terrorist Watchlist-Nominated Individuals

(U//~~FOUO~~) When a TWIC applicant's information results in a positive match to the Terrorist Watchlist, TSA officials contact the agency that nominated the applicant to obtain additional information to facilitate further vetting. Specifically, in cases where the FBI is the nominating agency, the TSA contacts FBI Headquarters personnel for information. Our review found that the FBI generally responded with information regarding [REDACTED]

[REDACTED] The FBI responds with a memorandum unless the individual is not under FBI investigation.²³ However, we found that the FBI did not document this process in its policies and procedures.

(S//~~NF~~//~~SSI~~) We reviewed [REDACTED] memoranda that involved FBI nominated individuals. We found that [REDACTED] of the memoranda [REDACTED]
[REDACTED]
[REDACTED]. In [REDACTED] of the [REDACTED] memoranda, the FBI responded that it had no objection to an action proposed by the TSA, which in [REDACTED] of the [REDACTED] memoranda was a [REDACTED]. In the remaining [REDACTED] of the [REDACTED] memoranda, the FBI stated that it took no position related to the watchlisted individual's credential.

²³ (U) The FBI also receives notifications of some positive Terrorist Watchlist matches for past TWIC applicants whose applications were denied, or whose TWIC cards have expired. In these cases, because the individuals have neither an active TWIC card nor a pending TWIC application, the FBI does not respond to the TSA with a memorandum.

(U//~~SSI~~) We further reviewed the [REDACTED] memoranda for the timeliness with which the FBI responded to the TSA. On average, the memoranda were dated [REDACTED] days after the TWIC encounter. There were [REDACTED] instances where the memoranda were dated [REDACTED] days or more after the encounter. Without a timely response from the FBI, watchlisted individuals who already have a TWIC retain access to secure Maritime facilities and vessels. We recommend that the FBI ensure timely responses to the TSA regarding its Terrorist Watchlist-nominated individuals to minimize the risk that these individuals pose to Maritime security.

(U//~~SSI~~) For [REDACTED], or approximately 23 percent, of the TWIC encounters relating to the FBI nominated individuals, we could not determine whether the FBI provided memoranda to the TSA. We recommend that the FBI retain its memoranda to the TSA to maintain a complete record of its communications and to ensure a more thorough record of actions related to its Terrorist Watchlist-nominated individuals.

(U) Encounters with Watchlisted Individuals Under FBI Investigation

(U//~~FOUO~~) We reviewed FBI documentation for [REDACTED] TWIC encounters with watchlisted individuals who were the subjects of an active FBI investigation at the time of the encounter. In [REDACTED] of these [REDACTED] instances, we found that the FBI

[REDACTED]
[REDACTED]. Based on our analysis, however, we have serious concerns that [REDACTED], FBI Case Agents were unaware of the risks posed by [REDACTED].

(U//~~FOUO~~//~~SSI~~) We interviewed a sample of Case Agents associated with 17 TWIC encounters. A third of these Case Agents were unaware of the vulnerabilities associated with the credential despite their involvement in investigations where the subject was attempting to obtain or renew a TWIC. Specifically, these Case Agents were unable to explain what a TWIC was and what access it granted, and they lacked other key information regarding the TWIC. Without knowledge of the TWIC, these Case Agents we interviewed could not have fully considered the impact of allowing an investigative subject continued access to secure Maritime areas. For example, one Case Agent expressed the concern that if [REDACTED], it would [REDACTED] and the [REDACTED] that could impede an investigation. But, the agent did not analyze whether the subject's [REDACTED] posed a risk of its own. Given this, the agents' concerns about potential impact to a pending FBI investigation could not be weighed in a meaningful way against the risks posed by a subject's access to secure Maritime facilities. Our review of FBI documentation found only [REDACTED] instances out of the [REDACTED] TWIC encounters reviewed where mitigating FBI actions, such as physical surveillance, were noted.

(U//~~FOUO~~) In addition, multiple Case Agents stated that they became aware that an investigative subject had a TWIC only after being notified by FBI

Headquarters personnel, or after they otherwise had a reason to check for the TWIC during the investigation, such as when the Case Agent learned that the subject was working in a Maritime facility. In May 2018, FBI officials stated that FBI Case Agents respond to TSA queries regarding subjects of FBI investigations based on their personal knowledge of their specific, individual investigations. Based on the interviews with FBI Case Agents conducted, we believe FBI Case Agents have responded to requests for information regarding [REDACTED] without having adequate information on the subject's use or need for the TWIC and the potential threat posed [REDACTED]. Educating FBI personnel on the TWIC will enable them to provide more informed responses to TSA about the risks associated with [REDACTED], and to better use TWIC data to gather evidence and intelligence in their investigations. We therefore recommend that the FBI increase its investigative personnel's awareness of the risks posed by the TWIC to the Maritime domain and the investigative data available from TWIC usage.

(U//~~FOUO~~) Additionally, most of these individuals were past or present subjects of FBI investigations at the time of the encounter and information was shared with FBI Headquarters and Case Agents. We found that this information was not disseminated to all FBI personnel that should have received it, such as MSP personnel, and that such a process was not included in its policies and procedures. In May 2017, an MSP official stated that MSP was not and would not be contacted in the event of a TWIC encounter and that he was unsure why the MSP would want this information. However, in May 2018, the FBI later provided information that, as of July 2016, the MSP utilized an embedded TSA analyst to track TWIC encounter information provided by [REDACTED]. Due to this conflicting information received, we believe that formalizing these procedures in a written format can prevent potential important national security information from being missed by the MSP. We believe that the information from encounters related to KST-TWIC applications or reinvestigations should be communicated to the MSP as the FBI's unit that has been tasked with preventing, penetrating, and dismantling acts of terrorism directed against Maritime assets. Providing this information to a centralized repository of Maritime-related intelligence, such as the MSP, can enhance the FBI's overall situational awareness of threats to the Maritime realm. Further, it ensures more timely and complete operational intelligence to MLAs in the field. We recommend that the FBI establish formalized procedures for communicating TWIC encounter information to the MSP to facilitate increased intelligence sharing and MSP identification of trends in the Maritime realm to help ensure greater protection of the nation's ports.

(U) Access to Secure Areas of Ports and Maritime Facilities

(U) There are over 350 ports in the United States, and each varies in its size, scope, and security needs. The TWIC is meant to provide some assurance that individuals issued the credential have been vetted for security risks. Private and public port ownership and management organizations rely on the TSA's TWIC applicant vetting process to conduct thorough background checks of individuals

seeking employment that requires unaccompanied access to secure areas at ports.²⁴

(U) The USCG, not the FBI, is responsible for the enforcement of the TWICs at the ports. According to a USCG final rule, effective August 2018, electronic inspection of TWICs is an important component of the USCG's "multi-layered system of access control requirements designed to enhance Maritime security."²⁵ However, the final rule requiring port card readers will apply only to Risk Group A vessels and facilities. Risk Group A consists of less than 5 percent of the MTSA-regulated population. The USCG final rule acknowledges that visual inspection does not address all security concerns and does not make full use of the security features contained in the TWIC. For instance, if a TWIC is stolen or lost, an unauthorized individual who resembles the picture on the TWIC could gain access to a secure area. Additionally, if an individual's TWIC privileges have been revoked or the TWIC card was deactivated, there is no way to ascertain that from a visual inspection of the credential. As noted earlier, there were 29 Guardian incidents related to lost, stolen, or counterfeit TWICs or unauthorized access with TWIC.

(U) According to the TWIC reader requirements final rule, as published in August 2016, the TWIC was being used only as a visual identity badge at many Maritime facilities. Once the credential is issued, the holder can continue to use it to access secure areas of vessels and facilities through a flash of the credential.²⁶ We asked the USCG for the number and location of ports with card readers and were told that, as of May 2017, the USCG did not have a list and lacked a central database with the most recent information.

(U) We also attempted to obtain information about the number, location, and use of card readers from local FBI MLAs. FBI MLAs establish and maintain working relationships with other local Maritime security stakeholders, such as DHS personnel, local law enforcement, and private industry personnel operating within ports. Some MLAs are involved in the development of the port security plans through MLA participation in Area Maritime Security Committees (AMSC), some participate in AMSC table-top exercises where a variety of port security scenarios are simulated, and some are members on AMSC subcommittees related to a variety of local port security concerns, such as cyber-security.²⁷

²⁴ (U) Port and facility owners may establish additional security measures at their facilities. As of April 2018, port card readers were not required by the USCG.

²⁵ (U) Transportation Worker Identification Credential (TWIC) – Reader Requirements, 81 Fed. Reg. 163, 57652 (Aug. 23, 2016). We note that a USCG threat analysis concluded that Risk Group A represents approximately 80 percent of the total Maritime security threat.

²⁶ (U) Auditors observed this visual inspection during a vessel familiarization tour of one port with FBI personnel.

²⁷ (U) USCG-organized AMSCs coordinate information sharing and other necessary activities to aid the security of the Marine Transportation System. AMSCs plan, develop, review, and update

(U//~~SSI~~) In response to our inquiries, we received information from [REDACTED] MLAs relating to ports within their areas of responsibility. According to these responses, the [REDACTED] have TWIC card readers at only a few facilities, and visual checks do not include physically inspecting the TWICs. At [REDACTED], the Port Administration and law enforcement are waiting for direction from the USCG regarding the TWIC reader issue. This response further included an MSP official's statement that, "some terminals within some ports have TWIC readers, and many do not," and that MLAs will not know the status of port card readers for all terminals within their ports.

(U) We also inquired during our audit about MSP management's attempts to visit a number of ports on an annual basis. During FYs 2013 and 2014, there were insufficient resources to conduct such port visits. The MSP resumed its port visits in FY 2015, at which time it began to conduct limited port visits in conjunction with other scheduled meetings, exercises, or conferences. In FY 2015, MSP personnel traveled to three ports: Los Angeles and San Diego, California; and New York City, New York. In FY 2016, MSP personnel traveled to six ports: New Orleans and Baton Rouge, Louisiana; San Juan, Puerto Rico; Savannah, Georgia; Houston, Texas; and Norfolk, Virginia. However, we found that the MSP lacked a methodology for strategically selecting which sites to visit.

(U) The main objective of MSP seaport visits is to meet local MLAs and FBI field office management to ascertain whether the MLAs are engaged with other Maritime security stakeholders and to obtain best practices. However, in January 2017, an FBI official stated that the MSP did not have a protocol for its port visits. We also found that the MSP's objectives for the port visits are often vague, and that its after-the-fact summaries of its visits often lacked specific findings and generally did not include overall conclusions or recommendations for improvement.

(U) We believe that port visits are an important element of the MSP's oversight responsibilities and that improvements can be made to the MSP's processes for selecting and scheduling port visits through the development of a methodology that could ensure consistency, effectiveness, and the efficient use of MSP's limited resources. One MSP official recognized this and stated that the FBI anticipates working to improve the objectives of these port visits. We recommend that the FBI establish clearer objectives for MSP's port visits, as well as a methodology for port visit selection, and guidance for how the visits should be used to increase the efficiency and effectiveness of, and to disseminate best practices concerning, port security.

(U) More generally, while the FBI does not control the implementation of port card readers, and is not responsible for the management or enforcement of the

Area Maritime Security Plans (AMSP) and enhance communication between Maritime stakeholders within federal, state and local agencies, and industry to address Maritime security issues. FBI MLAs are frequently involved in AMSCs. For example, the FBI co-chairs the AMSC with the USCG Captain of the Los Angeles-Long Beach Port Sector.

TWIC program, we believe the FBI, as an intelligence gathering entity and given its mission and function to protect the U.S. from terrorist threats, should take every opportunity to collect intelligence relating to the security of Maritime vessels and facilities. Maintaining better information about the implementation of the TWIC program, especially in locations where port access points are not secured with electronic verification through a card reader, is a critical component of the intelligence gathering and assessment process, and the FBI could better leverage its resources, including the MSP's port visits and MLA relationships with Maritime security stakeholders, to increase its intelligence gathering capability related to port security. Specifically, identifying ports where TWIC cards are only visually inspected raises the FBI's awareness of the increased security vulnerabilities related to unauthorized access, especially where watchlisted individuals are involved. We recommend that the FBI improve its intelligence collection by ensuring that MSP's port summary reports include information related to the port security, and disseminating this information to its MLAs.

(U) CONCLUSION AND RECOMMENDATIONS

(U) Key FBI counterterrorism officials told us that they consider the risk of terrorism to the Maritime domain to be low. However, our audit revealed that these officials may be relying on incomplete information when making this low risk determination. For example, we found that MSP did not identify all relevant information in Guardian that the FBI would need to fully assess the threat to the Maritime domain. While we only found a small number of instances where this occurred, any reliance on incomplete information can pose a significant threat to the Maritime domain. Additionally, we found that the FBI has not performed its own independent threat assessment for the Maritime domain. We believe an independent threat assessment by the FBI is warranted.

(U//~~FOUO~~//~~SSI~~) We also determined that TSA [REDACTED], and that in doing so they [REDACTED] from watchlisted individuals seeking a TWIC card. However, we believe [REDACTED] may have been made without an adequate understanding of the TWIC and the potential risks posed by a watchlisted individual possessing a TWIC.

(U) Finally, we found that MSP does not directly receive information related to TWIC encounters with watchlisted individuals, and is not fully aware of security measures used at ports, which prevents the MSP from using this information to identify security trends and most effectively carry out its intelligence gathering and sharing mission.

(U) We believe the weaknesses identified throughout this audit may create an environment in which the FBI could underestimate the risks, threats, and vulnerabilities to the Maritime domain, and miss opportunities to gather intelligence and take actions that could help to keep the nation's ports and Maritime assets safe.

(U) We recommend that the FBI:

1. (U) Conduct a full and independent evaluation, to be updated periodically, of the terrorism threat to the Maritime domain with resulting intelligence product(s) disseminated to key stakeholders.
2. (U) Document the policies and procedures MSP personnel utilize to complete their Intelligence Summary Reports, such as listings of keyword searches and distribution lists, to ensure continuity of operations within the MSP and to ensure dissemination of the most thorough Maritime-related intelligence to field personnel.
3. (U) Strengthen its policies and procedures for working with the TSA to enhance the vetting and scrutiny of No Fly TWIC applicants and cardholders.

4. (U) Ensure timely responses to the TSA regarding its Terrorist Watchlist-nominated individuals to minimize the risk that these individuals pose to Maritime security.
5. (U) Retain its memoranda to the TSA to maintain a complete record of its communications and to ensure a more thorough record of actions related to its Terrorist Watchlist-nominated individuals.
6. (U) Increase its investigative personnel's awareness of the risks posed by the TWIC to the Maritime domain and the investigative data available from TWIC usage.
7. (U) Establish formalized procedures for communicating TWIC encounter information to the MSP to facilitate increased intelligence sharing and MSP identification of trends in the Maritime realm to help ensure greater protection of the nation's ports.
8. (U) Establish clearer objectives for MSP's port visits, as well as a methodology for port visit selection, and guidance for how the visits should be used to increase the efficiency and effectiveness of, and to disseminate best practices concerning, port security.
9. (U) Improve its intelligence collection by ensuring that MSP's port summary reports include information related to the port security, and disseminating this information to its MLAs.

(U) STATEMENT ON INTERNAL CONTROLS

(U) As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of the FBI's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. The FBI's management is responsible for the establishment and maintenance of internal controls.

(U) As noted in the Audit Results section of this report, we identified certain deficiencies in the FBI's internal controls that we believe adversely affect the FBI's ability to identify and review all Maritime-related threats.

(U) Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

(U) STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

(U) As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices, to obtain reasonable assurance that the FBI's management complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on the results of our audit. FBI management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the FBI and that were significant within the context of the audit objectives:

- (U) Maritime Transportation Security Act of 2002, Pub. L. 107-295 (2002)
- (U) Transportation Worker Identification Credential (TWIC) – Reader Requirements final rule, 81 Federal Register 57652, August 23, 2016
- (U) Homeland Security Presidential Directive-6, September 2003
- (U) Homeland Security Presidential Directive-13, December 2004

(U) Our audit included examining, on a test basis, the FBI's compliance with laws and regulations that could have a material effect on the FBI's operations. We interviewed auditee personnel, analyzed data, and examined procedural practices. Nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned laws and regulations.

APPENDIX 1**(U) OBJECTIVES, SCOPE, AND METHODOLOGY****(U) Objectives**

(U) The objectives of the audit were to review the FBI's roles and responsibilities for: (1) assessing Maritime terrorism threats and (2) coordinating with the Department of Homeland Security (DHS) components in ensuring seaport security. The scope of this audit, unless otherwise stated, generally focused on activities from October 2012 through July 2017.

(U) Scope and Methodology

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) To accomplish the audit objectives, we reviewed various laws and policies including 18 U.S.C. § 7, the Maritime Transportation Security Act of 2002, 81 Federal Register 57652, and the Homeland Security Presidential Directive-6. We also interviewed personnel from the FBI at the headquarters and local levels. Within the FBI, we spoke with personnel from the following components: Maritime Security Program (MSP), Guardian Management Unit, Domestic Terrorism Operations Unit, International Terrorism Operations Unit, Terrorist Financing Operations Section, Criminal Investigative Division, Directorate of Intelligence Division, Office of Personnel Engagement, Hostage Rescue Team, and the Critical Incident Response Group. We also spoke with Case Agents across different field offices and FBI Maritime Liaison Agents in Long Beach, Monterey, and San Francisco, California. We also reviewed Intelligence Summary Reports, port visit summaries, and other documentation relating to MSP's operations and FBI Maritime capabilities.

(U) To assess the FBI's coordination with DHS components, we spoke with personnel from the U.S. Coast Guard (USCG) and Customs and Border Protection. Notably, entities within these components at the headquarters level included: Coastwatch, the Information and Incident Coordination Unit, the National Targeting Center, and the Air and Marine Operations Center. Beyond these components, we interviewed personnel from the Global Maritime Operational Threat Response Coordination Center. We also spoke to the Captain of the Port of San Francisco and other local USCG personnel in the San Francisco area. From the USCG we requested and reviewed documents relating to its risk assessments. Further, in

light of the responsibilities of TSA, USCG, and CBP in the Maritime domain, we have shared the findings and conclusions of this audit with our counterparts at DHS OIG periodically throughout the audit.

(U) For our review of the Transportation Worker Identification Credential (TWIC), we obtained a list of positive encounters related to the TWIC from the FBI. We interviewed personnel in the Transportation Security Administration's TWIC Program Management Office and Office of Intelligence and Analysis. We also requested and reviewed TWIC data and related documentation from the TSA. We further obtained and reviewed the FBI Terrorist Screening Center's positive encounter records related to KSTs' TWIC applications and portions of Sentinel cases and Guardian incident assessments related to these encounters. We also interviewed personnel from different units within the TSC, including the TSC's Chief Counsel. TWIC information obtained was dated between January 2008 and July 2017.

APPENDIX 2

(U) TWIC DISQUALIFYING OFFENSES

Part A: PERMANENT DISQUALIFYING CRIMINAL OFFENSES	
1.	Espionage or conspiracy to commit espionage
2.	Sedition or conspiracy to commit sedition
3.	Treason or conspiracy to commit treason
4.	A federal crime of terrorism as defined in 18 U.S.C. § 2332b(g), or comparable State law, or conspiracy to commit such crime
5.	A crime involving a TSI (transportation security incident). Note: A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. § 70101
6.	Improper transportation of a hazardous material under 49 U.S.C. § 5124 or a comparable state law
7.	Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device
8.	Murder
9.	Threat or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility
10.	Violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act, 18 U.S.C. § 1961, et seq., or a comparable State law, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the permanently disqualifying crimes
11.	Attempt to commit the crimes in items (1)-(4) of this section
12.	Conspiracy or attempt to commit the crimes in items (5)-(10) of this section
Part B: INTERIM DISQUALIFYING CRIMINAL OFFENSES	
1.	Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. § 921(a)(3) or 26 U.S.C. § 5845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21
2.	Extortion
3.	Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering, where the money laundering is related to a crime listed in Parts A or B (except welfare fraud and passing bad checks)
4.	Bribery
5.	Smuggling
6.	Immigration violations
7.	Distribution, possession with intent to distribute, or importation of a controlled substance
8.	Arson
9.	Kidnapping or hostage taking
10.	Rape or aggravated sexual abuse
11.	Assault with intent to kill
12.	Robbery
13.	Fraudulent entry into a seaport as described in 18 U.S.C. 1036, or a comparable State law
14.	Violations of the RICO Act under 18 U.S.C. § 1961, et seq., or a comparable state law, other than any permanently disqualifying offenses
15.	Voluntary manslaughter
16.	Conspiracy or attempt to commit crimes in this section
Part C: UNDER WANT, WARRANT OR INDICTMENT	
A person will be disqualified if he or she is wanted or under indictment in any civilian or military jurisdiction for a felony listed under Part A or Part B until the want or warrant is released or the indictment is dismissed	

APPENDIX 3

(U) LIST OF KEYWORDS FOR MSP SEARCHES

(U) The FBI's MSP provided the following list of keywords that its Analysts use in searching databases:

Absconder
Boat
Cargo Ship*
Coast Guard
Container Ship*
Crew member
Crewmember
Cruise ship
Dock
Ferry
Maritime
MV²⁸
Port of
Seaport
Scuba
Ship
Submersible*
TWIC*
USCG
Vessel

* New keywords on MSP's list provided in February 2018.

²⁸ (U) "MV" stands for Motor Vessel.

APPENDIX 4

(U) THE FEDERAL BUREAU OF INVESTIGATION'S RESPONSE
TO THE DRAFT REPORT



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 30, 2018

(U) The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

(U) Dear Mr. Horowitz:

(U) The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats*.

(U) We agree that it is important to enhance protocols and procedures for working with DHS' Transportation Security Administration to improve communication and information sharing related to Transportation Worker Identification Credentials. In that regard, we concur with your nine recommendations for the FBI.

(U) Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

(U) Sincerely,

A handwritten signature in black ink, appearing to read "Tom Seiler", is written over the typed name.

(U) Thomas G. Seiler
Acting Section Chief
External Audit and Compliance Section
Inspection Division

(U) Enclosure

**(U) The Federal Bureau of Investigation's Response to the
Office of the Inspector General's Audit of the FBI's Management of Maritime Terrorism Threats**

- (U) Draft Report Recommendation #1:** Conduct a full and independent evaluation, to be updated periodically, of the terrorism threat to the Maritime domain with resulting intelligence product(s) disseminated to key stakeholders.
- (U) FBI Response to Recommendation #1: Concur.** FBI will collaborate as necessary to establish a baseline intelligence product providing an evaluation of the current and recent terrorism threat to the maritime domain for future periodic update and dissemination to stakeholders.

- (U) Draft Report Recommendation #2:** Document the policies and procedures MSP personnel utilize to complete their Intelligence Summary Reports, such as listing of keyword searches and distribution lists, to ensure continuity of operations within the MSP and to ensure dissemination of the most thorough Maritime-related intelligence to field personnel.
- (U) FBI Response to Recommendation #2: Concur.** FBI will formally document policies and procedures used by MSP personnel to complete MSP Intelligence Summary Reports, establish a baseline of intelligence products with a focus on maritime domain related information, and document the process for dissemination of the summary.

- (U) Draft Report Recommendation #3:** Strengthen its policies and procedures for working with the TSA to enhance the vetting and scrutiny of No Fly TWIC applicants and cardholders.
- (U) FBI Response to Recommendation #3: Concur.** The FBI will strengthen its policies and procedures for working with the TSA to enhance the vetting and scrutiny of No Fly TWIC applicants and cardholders.

- (U) Draft Report Recommendation #4:** Ensure timely responses to the TSA regarding its Terrorist Watchlist-nominated individuals to minimize the risk that these individuals pose to Maritime security.
- (U) FBI Response to Recommendation #4: Concur.** The FBI will continue to ensure timely responses to the TSA liaison.

- (U) Draft Report Recommendation #5:** Retain its memoranda to the TSA to maintain a complete record of its communications and to ensure a more thorough record of actions related to its Terrorist Watchlist-nominated individuals.
- (U) FBI Response to Recommendation #5: Concur.** The FBI will retain its memoranda to maintain a complete record of its communications and to ensure a more thorough record of actions related to its Terrorist Watchlist-nominated individuals.

- (U) **Draft Report Recommendation #6:** Increase its investigative personnel's awareness of the risks posed by the TWIC to the Maritime domain and the investigative data available from TWIC usage.
- (U) **FBI Response to Recommendation #6: Concur.** The FBI will obtain additional training for headquarters MSP personnel and field office Maritime Liaison Agents regarding USCG security requirements and the TSA TWIC program. We will also coordinate with TSA regarding enhanced vetting of TWIC holders for the overall security of the Maritime domain.
- (U) **Draft Report Recommendation #7:** Establish formalized procedures for communicating TWIC encounter information to the MSP to facilitate increased intelligence sharing and MSP identification of trends in the Maritime realm to help ensure greater protection of the nation's ports.
- (U) **FBI Response to Recommendation #7: Concur.** The FBI will coordinate with the various divisions impacted to formalize procedures to communicate TWIC encounter information.
- (U) **Draft Report Recommendation #8:** Establish clearer objectives for MSP's port visits, as well as a methodology for port visit selection, and guidance for how the visits should be used to increase the efficiency and effectiveness of, and to disseminate best practices concerning, port security.
- (U) **FBI Response to Recommendation #8: Concur.** The FBI will document the objectives and methodology for port visit selection, and guidance for how the visits should be used to increase the efficiency and effectiveness of, and to disseminate best practices concerning, port security.
- (U) **Draft Report Recommendation #9:** Improve its intelligence collection by ensuring that MSP's port summary reports include information related to the port security, and disseminating this information to its MLAs.
- (U) **FBI Response to Recommendation #9: Concur.** The FBI will document the objectives and methodology for port visit selection. MSP will also document and disseminate guidance on the purpose, scope, and utility of port visits and the requirements for port summary reports for all MLAs.

APPENDIX 5

**(U) OFFICE OF THE INSPECTOR GENERAL
ANALYSIS AND SUMMARY OF ACTIONS
NECESSARY TO CLOSE THE REPORT**

(U) The OIG provided a draft of this audit report to the FBI. The FBI response is incorporated in Appendix 4 of this final report. In response to our audit report, the FBI concurred with our recommendations and discussed the actions it will implement in response to our findings. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

(U) Recommendation for the FBI:

1. **(U) Conduct a full and independent evaluation, to be updated periodically, of the terrorism threat to the Maritime domain with resulting intelligence product(s) disseminated to key stakeholders.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will create a baseline intelligence product providing an evaluation of the current and recent terrorism threat to the Maritime domain for future periodic update and dissemination to stakeholders. This recommendation can be closed when we receive evidence and dissemination of the baseline intelligence product, as well as plans for its update and future dissemination.

2. **(U) Document the policies and procedures MSP personnel utilize to complete their Intelligence Summary Reports, such as listings of keyword searches and distribution lists, to ensure continuity of operations within the MSP and to ensure dissemination of the most thorough Maritime-related intelligence to field personnel.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will formally document policies and procedures used by MSP personnel to complete MSP Intelligence Summary Reports, establish a baseline of intelligence products focusing on Maritime domain related information, and document the process for dissemination of the summary. This recommendation can be closed when we receive documentation of its policies and procedures and evidence of its implementation.

3. **(U) Strengthen its policies and procedures for working with the TSA to enhance the vetting and scrutiny of No Fly TWIC applicants and cardholders.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will strengthen policies and procedures regarding its coordination with the TSA to enhance the vetting and scrutiny of No Fly TWIC applicants and cardholders. This recommendation can be closed when we receive documentation and implementation of these improved policies and procedures.

4. **(U) Ensure timely responses to the TSA regarding its Terrorist Watchlist-nominated individuals to minimize the risk that these individuals pose to Maritime security.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will continue to ensure that it responds timely to the TSA liaison. This recommendation can be closed when we receive evidence of its timely responses to the TSA.

5. **(U) Retain its memoranda to the TSA to maintain a complete record of its communications and to ensure a more thorough record of actions related to its Terrorist Watchlist-nominated individuals.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will maintain a complete record of its communication and ensure a more thorough record of activity on its Terrorist Watchlist-nominated individuals by retaining its memoranda. This recommendation can be closed when we receive evidence that the FBI has developed and implemented a procedure to ensure that these memoranda are maintained.

6. **(U) Increase its investigative personnel's awareness of the risks posed by the TWIC to the Maritime domain and the investigative data available from TWIC usage.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will obtain training on USCG security requirements and the TSA TWIC program for its headquarters MSP personnel and field office Maritime Liaison Agents. The FBI also stated that it will work with the TSA to enhance vetting of TWIC holders for overall security in the Maritime domain. This recommendation can be closed when we receive evidence that training regarding TSA TWIC program and investigate data from TWIC usage has been provided to all MSP and field office Maritime Liaison Agents.

7. **(U) Establish formalized procedures for communicating TWIC encounter information to the MSP to facilitate increased intelligence sharing and MSP identification of trends in the Maritime realm to help ensure greater protection of the nation's ports.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will coordinate with the various divisions impacted to formalize procedures to communicate TWIC encounter information. This recommendation can be closed when we receive evidence and implementation of its formalized procedures regarding communication of TWIC encounter information to the MSP.

8. **(U) Establish clearer objectives for MSP's port visits, as well as a methodology for port visit selection, and guidance for how the visits should be used to increase the efficiency and effectiveness of, and to disseminate best practices concerning, port security.**

(U) Resolved. The FBI concurred with our recommendation. The FBI stated in its response that it will document the objectives and methodology for port visit selection, guidance for how the visits should be used to increase the efficiency and effectiveness of, and to disseminate best practices concerning, port security. This recommendation can be closed when we receive documentation and implementation of MSP's port visits objectives, port selection methodology, and guidance for how the visits should be used to increase the efficiency and effectiveness of port security as well as the dissemination of port security best practices developed from MSP's port visits.

9. **(U) Improve its intelligence collection by ensuring that MSP's port summary reports include information related to the port security, and disseminating this information to its MLAs.**

(U) Resolved. The FBI concurred with our recommendation. The FBI reiterated that it will document the objectives and selection methodology of its port visits. The FBI also stated in its response that the MSP will document and issue guidance discussing the purpose, scope, and utility of the port visits and the content requirements for the resulting port summary reports for all MLAs. This recommendation can be closed when we receive documentation and of the FBI's guidance on MSP's port visits and port summary reports and evidence of its dissemination of the information to the MLAs.



The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL

950 Pennsylvania Avenue, Northwest
Suite 4760
Washington, DC 20530 0001

Website	Twitter	YouTube
oig.justice.gov	@JusticeOIG	JusticeOIG

Also at Oversight.gov